Brittany Resch (*pro hac vice*)
Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
bresch@straussborrelli.com
raina@straussborrelli.com

Andrew W. Ferich (*pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Anthony L. Parkhill (*pro hac vice*)
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
aparkhill@barnowlaw.com

Proposed Interim Class Counsel
[Additional Counsel Appear on Signature Page]

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

LAZARO STERN, CELESTE ALLEN, LISA KUCHERRY, PETER SMITH, and SHARON THOMPSON, individually and on behalf of all others similarly situated, Plaintiffs, v. ACADEMY MORTGAGE CORPORATION, Defendant.	Case No. 2:24-cv-00015-DBB-DAO **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED Judge David Barlow

Plaintiffs Lazaro Stern, Celeste Allen, Lisa Kucherry, Peter Smith, and Sharon Thompson ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class

members"), by and through their attorneys, bring this Amended Class Action Complaint against Defendant Academy Mortgage Corporation ("Academy" or "Defendant") and complain and allege upon personal knowledge as to themselves and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Academy for its failure to secure and safeguard their and approximately 284,443 other individuals' personally identifiable information ("PII"), including first and last names, dates of birth, and Social Security numbers.

2. Academy is an independent mortgage lender based in Draper, Utah. Academy offers a wide range of consumer mortgage options, including conventional loans, FHA loans, VA loans, USDA loans, jumbo loans, renovation loans, and other refinancing options. Academy touts itself as one of the top independent purchase lenders in the country.

3. On or about March 21, 2023, Academy discovered that it had lost control over its computer network and the highly sensitive PII stored therein. It reported a network security incident in which "an unauthorized third party accessed and disabled some of [its] systems," and responded by launching an internal investigation into the suspicious activity.[1] Academy's investigation revealed that one or more unauthorized individuals gained access to Academy's network systems and accessed certain files containing the sensitive personal information of Academy's current and former customers and employees (the "Data Breach").

4. Critically, as described *infra*, the notorious cybercriminal group "ALPHV BlackCat" revealed that it had accessed and exfiltrated PII from Academy during the Data Breach.

[1] Academy Mortgage Corporation, *Notice of Data Security Incident*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/203fc6cf-82c9-4d8e-b280-501bb49c6602/0f945733-a56e-44d3-8ea8-a03e343a46d4/Academy%20Sample%20Notifications.pdf (last accessed Feb. 20, 2025).

To make matters worse, on or around May 14, 2023, ALPHV BlackCat then ***published*** stolen PII on the Dark Web. Thereafter, other cybercriminal groups gained actual and immediate access to such stolen PII. Because the PII is published on the Dark Web, it is available for anyone to access, view, obtain, and use to commit a host of crimes. Plaintiffs and Class Members have already suffered from the actual misuse of their PII by cybercriminals (i.e., ALPHV BlackCat).

5. Academy provided limited details about the Data Breach, failing to include whether or not the cybercriminal(s) responsible for the Data Breach were identified or whether the information exfiltrated was held for ransom. Academy also did not disclose whether its investigation detected the compromised information on the dark web. Instead, Academy stated that it "wiped and rebuilt affected systems and [has] taken steps to bolster [its] network security."

6. Despite learning of the Data Breach as early as March 21, 2023, Academy did not announce the Data Breach publicly until nine months later, on or around December 20, 2023, and did not begin sending out Data Breach notification letters to affected individuals until around that time. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII. This is especially harmful because the cybercriminals who perpetrated the Data Breach had already released Plaintiffs' and Class members' PII onto the dark web.

7. Academy's Notice also did not disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanism of the cyberattack, the reason for the delay in notifying Plaintiffs and the Class members of the Data Breach, how Academy determined

that the PII had been "accessed" by an unauthorized party, that their PII was now on the dark web, and, importantly, what specific steps Academy took following the Data Breach to secure its systems and prevent future cyberattacks.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack. Cybercriminals were able to breach Defendant's systems because of these failures, and because Defendant failed to adequately train its employees on cybersecurity, and failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiffs and Class members.

9. By being entrusted with Plaintiffs' and Class members' PII for its own pecuniary benefit, Defendant assumed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class members' PII against unauthorized access and disclosure. Defendant also had a duty to adequately safeguard this PII under applicable law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act") and the Gramm-Leach-Bliley Act. Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession from unauthorized access and disclosure.

10. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on

proper security measures; and failing to provide Plaintiffs and Class members prompt and adequate notice of the Data Breach.

11. Further, Defendant maintained, used, and shared the PII it obtained in a reckless manner. In particular, the PII was used and transmitted by Defendant in a condition vulnerable to cyberattacks. The potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left Plaintiffs and Class members vulnerable.

12. In addition, Defendant failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

13. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs and approximately 284,443 Class members suffered injury and ascertainable losses in the form of their information being released on the dark web, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from their exposure, and the present and imminent threat of fraud and identity theft.

14. These losses are exacerbated by the fact that Plaintiffs and Class members' PII remains unencrypted and available for unauthorized third parties to access and abuse. Their PII also remains backed up in Defendant's possession, which means Plaintiffs and Class members' PII is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. The security of Plaintiffs' and Class members' identities is now at risk because of Defendant's wrongful conduct, as the PII that Defendant collected and maintained is now in the

hands of data thieves and has been released on the dark web. This present risk will continue for the course of their lives.

16. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class members' names, taking out loans in their names, using their identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class members' names, and giving false information to police during an arrest.

17. As a result of the Data Breach, Plaintiffs and Class members have been exposed to a present and imminent risk of fraud and identity theft, especially in light of the fact that their PII has been released on the dark web. Among other measures, Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiffs and Class members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiffs and Class members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because the exposed information includes Social Security numbers and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

19. Plaintiffs bring this action on behalf of themselves and all individuals in the United States whose PII was exposed as a result of the Data Breach Defendant learned of on or about March 21, 2023, and first publicly acknowledged on or about December 20, 2023. Plaintiffs and Class members seek to hold Defendant responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiffs seek to remedy the

harms resulting from the Data Breach on behalf of themselves and all similarly situated individuals whose PII was accessed and exfiltrated during the Data Breach.

20. Plaintiffs, on behalf of themselves and all other Class members, bring claims for negligence, breach of implied contract, unjust enrichment, violation of the Washington Consumer Protection Act, and violation of the Idaho Consumer Protection Act, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and Class members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

21. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the PII of Plaintiffs and the Class members was exactly that—private. Now, their PII is permanently exposed and unsecure.

PARTIES

Plaintiff Lazaro Stern

22. Plaintiff Lazaro Stern is a resident of the state of Florida.

23. Plaintiff Stern is a former customer of Defendant. He provided his PII to, or otherwise had his PII provided to, Academy when he took a mortgage with Academy in 2013. Academy used his PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain its mortgage services.

24. Plaintiff received a letter from Academy notifying him that he was affected by the Data Breach on or around December 23-24, 2023.

25. Plaintiff provided his PII to Academy and trusted that it would use reasonable measures to protect his PII according to state and federal law. Had Plaintiff known that Academy does not adequately protect PII, he would not have used Academy's services and agreed to provide Academy with his PII.

26. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had she known of Defendant's lax data security policies.

27. As a result of its inadequate cybersecurity, Defendant exposed Plaintiffs' PII for theft by cybercriminals and sale on the dark web.

28. Plaintiff does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

29. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect. Such damages and diminutions are heightened substantially because ALPHV BlackCat already published stolen PII on the Dark Web.

30. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring his credit information. These efforts were reasonable and necessary given that ALPHV BlackCat already published stolen PII on the Dark Web.

31. Plaintiff has already spent and will continue to spend considerable time and effort

monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security, especially due to the uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These emotional injuries were caused by Plaintiff's exposure to a heightened risk—of identity theft and fraud—which has been substantially elevated because ALPHV BlackCat already published stolen PII on the Dark Web.

32. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach. This risk is acutely high because ALPHV BlackCat already published stolen PII on the Dark Web.

33. Indeed, following the breach, Mr. Stern started receiving text messages related to taking out lines of credit. Plaintiff has also experienced an enormous increase in spam calls, up to ten a day, all of this suggesting that his PII is now in the hands of cybercriminals.

34. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Celeste Allen

35. Plaintiff Celeste Allen is a resident of the state of Washington.

36. Plaintiff Allen is a former customer of Defendant, using Academy as her lender in 2017 and 2020. She provided her PII to, or otherwise had her PII provided to, Academy in

connection with transaction or seeking lending services from Academy. Academy used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain its mortgage services.

37. Plaintiff received a letter from Academy notifying her that she was affected by the Data Breach in or around December 2023.

38. Plaintiff provided her PII to Academy and trusted that it would use reasonable measures to protect her PII according to state and federal law. Had Plaintiff known that Academy does not adequately protect PII, she would not have used Academy's services and agreed to provide Academy with her PII.

39. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

40. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

41. Plaintiff suffered actual and concrete injury, including actual exposure and misuse, the loss of control over her PII, the diminished value of her personal data, and the substantial risk of fraudulent use. After all, PII is a form of intangible property—property that Defendant was required to adequately protect. Such damages and diminutions are heightened substantially because ALPHV BlackCat already published stolen PII on the Dark Web. This, itself, is misuse of PII. Plaintiff's PII is now available on the Dark Web, where it has been exposed to the public and is now accessible to cybercriminals and identity thieves.

42. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts

to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring her credit information. These efforts were reasonable and necessary given that ALPHV BlackCat already published stolen PII on the Dark Web, and such efforts have imposed significant and quantifiable financial and other burdens on Plaintiff.

43. Plaintiff has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security, especially due to the uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These emotional injuries were caused by Plaintiff's exposure to a heightened risk—of identity theft and fraud—which has been substantially elevated because ALPHV BlackCat already published stolen PII on the Dark Web.

44. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her exposed PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach. This risk is acutely high because ALPHV BlackCat already published stolen PII on the Dark Web.

45. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls, suggesting that her PII is now in the hands of cybercriminals.

46. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Lisa Kucherry

47. Plaintiff Lisa Kucherry is a resident of the state of Idaho.

48. Plaintiff Kucherry is a former customer of Defendant. She provided her PII to, or otherwise had her PII provided to, Academy in connection with seeking lending services from Academy. Academy used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain its mortgage services.

49. Plaintiff received a letter from Academy notifying her that she was affected by the Data Breach on or around December 20, 2023.

50. Plaintiff provided her PII to Academy and trusted that it would use reasonable measures to protect her PII according to state and federal law. Had Plaintiff known that Academy does not adequately protect PII, she would not have used Academy's services and agreed to provide Academy with her PII.

51. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

52. As a result of its inadequate cybersecurity, Defendant exposed Plaintiffs' PII for theft by cybercriminals and sale on the dark web.

53. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was

required to adequately protect. Such damages and diminutions are heightened substantially because ALPHV BlackCat already published stolen PII on the Dark Web.

54. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, signing up for the credit monitoring services offered by Defendant, and monitoring her financial accounts for any unusual activity. These efforts were reasonable and necessary given that ALPHV BlackCat already published stolen PII on the Dark Web.

55. Plaintiff has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security, especially due to the uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These emotional injuries were caused by Plaintiff's exposure to a heightened risk—of identity theft and fraud—which has been substantially elevated because ALPHV BlackCat already published stolen PII on the Dark Web.

56. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach. This risk is acutely high because ALPHV BlackCat already published stolen PII on the Dark Web.

57. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls, suggesting that her PII is now in the hands of cybercriminals.

58. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Peter Smith

59. Plaintiff Peter Smith is a resident of the state of Washington.

60. Plaintiff Smith is a former customer of Defendant. He provided his and his spouse's PII to, or otherwise had their PII provided to, Academy when he had his mortgage appraised with Academy in February 2021. Academy used his PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain its mortgage services.

61. Plaintiff received a letter from Academy notifying him that he was affected by the Data Breach on or around December 20, 2023.

62. Plaintiff provided his PII to Academy and trusted that it would use reasonable measures to protect his PII according to state and federal law. Had Plaintiff known that Academy does not adequately protect PII, he would not have used Academy's services and agreed to provide Academy with his PII.

63. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had she known of Defendant's lax data security policies.

64. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

65. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was

required to adequately protect. Such damages and diminutions are heightened substantially because ALPHV BlackCat already published stolen PII on the Dark Web.

66. Indeed, following the breach, Mr. Smith had his identity stolen—someone took out a loan through Credit First using Mr. Smith's identity. The loan was initially $8200 but the balance eventually reached $9225. His credit report indicates the loan was taken out on April 21, 2023—at least one month after Defendant's breach and seven months before Plaintiff received his notice of breach letter from Defendant.

67. On information and belief, ALPHV BlackCat was responsible for this fraudulent loan—and used the PII that ALPHV BlackCat had exfiltrated from Academy during the Data Breach in March 2023.

68. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to speaking with Credit First about the fraudulent loan, filing a police report, filing a report with the FTC, researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring his credit information. These efforts were reasonable and necessary given that ALPHV BlackCat already published stolen PII on the Dark Web.

69. Plaintiff has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security, especially due to the actual fraudulent use of his PII. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These emotional

injuries were caused by Plaintiff's exposure to a heightened risk—of identity theft and fraud—which has been substantially elevated because ALPHV BlackCat already published stolen PII on the Dark Web.

70. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach. This risk is acutely high because ALPHV BlackCat already published stolen PII on the Dark Web.

71. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Sharon Thompson

72. Plaintiff Sharon Thompson is a resident of the state of Georgia.

73. Plaintiff Thompson is a former employee of Defendant, where she worked as a mortgage originator from 2017 to 2020. She provided her PII to, or otherwise had her PII provided to, Academy in connection with her employment. Academy used that PII to facilitate its hiring and provision of benefits to Plaintiff and required Plaintiff to provide that PII to obtain and maintain employment. Academy continued to maintain her PII long after her employment ended.

74. Plaintiff received a letter from Academy notifying her that she was affected by the Data Breach on or around December 20, 2023.

75. Plaintiff provided her PII to Academy and trusted that it would use reasonable measures to protect her PII according to state and federal law. Had Plaintiff known that Academy does not adequately protect PII, she would not have sought employment with Academy and agreed

to provide Academy with her PII.

76. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

77. As a result of its inadequate cybersecurity, Defendant exposed Plaintiffs' PII for theft by cybercriminals and sale on the dark web.

78. Plaintiff does not recall ever learning that her PII was compromised in a data breach incident before learning about the breach at issue in this case.

79. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect. Such damages and diminutions are heightened substantially because ALPHV BlackCat already published stolen PII on the Dark Web.

80. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information. These efforts were reasonable and necessary given that ALPHV BlackCat already published stolen PII on the Dark Web.

81. Plaintiff has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security, especially due to the uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it

is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These emotional injuries were caused by Plaintiff's exposure to a heightened risk—of identity theft and fraud—which has been substantially elevated because ALPHV BlackCat already published stolen PII on the Dark Web.

82. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach. This risk is acutely high because ALPHV BlackCat already published stolen PII on the Dark Web.

83. Indeed, following the Data Breach, Plaintiff has experienced a significant increase in spam calls, suggesting that her PII is now in the hands of cybercriminals.

84. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant Academy Mortgage Corporation

85. Defendant Academy Mortgage Corporation is incorporated in Utah, with its principal place of business at 339 West 13490 South, Draper, Utah 84020. Defendant can be served through its registered agent, Corporation Service Company at 15 West South Temple, Suite 600 Salt Lake City, Utah 84101.

JURISDICTION AND VENUE

86. This Court has jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000,

exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the proposed class is a citizen of a different state than Defendant.

87. This Court has personal jurisdiction over Defendant because Academy is a corporation organized under the laws of Utah and has its principal place of business at 339 West 13490 South, Draper, Utah 84020. Additionally, the acts and omissions giving rise to Plaintiffs' claims occurred and/or emanated from this District.

88. Venue is proper in this District because Academy maintains its headquarters and principal place of business in this District.

FACTUAL ALLEGATIONS

Overview of Academy Mortgage Corporation

89. Founded in 1988, Academy is an independent mortgage lender based in Draper, Utah. Academy offers a wide range of consumer mortgage options, including conventional loans, FHA loans, VA loans, USDA loans, jumbo loans, renovation loans, and other refinancing options.[2]

90. Academy touts itself as "recognized and respected nationwide" for providing "exceptional service and the best solutions and tools to help individuals and families achieve successful homeownership."[3] It is reported as having made over $35 million in annual revenue in 2023.[4]

91. In the regular course of its business, Academy collects and maintains the PII of customers, employees, and other persons who otherwise are affiliated or transacted with Academy for business purposes.

---

[2] *See* https://academymortgage.com/about (last accessed Jan. 25, 2024).
[3] Academy Mortgage Corporation, Linkedin, https://www.linkedin.com/company/academy-mortgage-corporation/ (last accessed Feb. 20, 2025).
[4] Academy Mortgage Corporation, Zippia, https://www.zippia.com/academy-mortgage-careers-13386/revenue/ (last accessed Feb. 20, 2025).

92. Academy requires customers and employees to provide their highly sensitive personally identifiable information to facilitate its mortgage services.[5] That information includes, but is not limited to, an individual's first and last name, address, e-mail address, phone number, Social Security number, credit scores and credit history, and financial information—such as income, assets, and liabilities, information about the individual's savings, investments, insurance, and business.[6] Academy stores this information digitally.

93. In collecting and maintaining PII, Academy implicitly agreed that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

94. Academy's Privacy Policy ensures customers and other related persons that it is "committed to ensuring that your information is secure" and it "use[s] commercially reasonable efforts to protect your personal information collected, used, stored, shared, or transferred as part of [its] Services from access, loss, misuse, alteration, or destruction by any unauthorized party."[7] It further states, "Academy protects data using administrative, technical, and physical safeguards" and that "when [it] use[s] third-party service providers, [it] ask[s] those providers to implement similar safeguards."[8]

95. Despite recognizing its duty to do so, Academy has not implemented reasonable cybersecurity safeguards or policies to protect consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Academy has significant vulnerabilities in its systems that cybercriminals can exploit to gain access to consumers' PII.

[5] *See* https://academymortgage.com/privacy-policy (last accessed June 16, 2024).
[6] *Id.*
[7] *Id.*
[8] *Id.*

96. By obtaining, collecting, using, and benefitting from Plaintiffs' and Class member's PII, Defendant assumed legal and equitable duties that required Defendant to, at a minimum, implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

97. Plaintiffs and Class members are, or were, customers or employees of Defendant, or otherwise are affiliated or transacted with Defendant and entrusted Defendant with their PII.

98. Plaintiffs and Class members reasonably relied on Academy's representations regarding data security, and on Defendant to maintain the confidentiality and security of their PII and only to make required, authorized disclosures of this information, which Defendant ultimately failed to do. Compounding Defendant's breach of these duties, Defendant waited approximately nine months after discovering the Data Breach to notify those affected that their PII had been compromised.

The Data Breach

99. On or about March 21, 2023, Academy discovered that an unauthorized third party, gained access to and disabled Academy's network systems. Academy has not revealed how long cybercriminals may have had access to its network.

100. Academy did not publicly announce the Data Breach until about December 20, 2023, when it began sending letters notifying customers of the Data Breach (the "Notice Letters"). The Notice Letters that Academy sent to Plaintiffs and the Class stated that the company detected the "network security incident" on March 21, 2023, which it described as "an unauthorized third party accessed and disabled some of our systems."[9] But this is far from the truth. Academy

[9] *Notice of Data Security Incident*, *supra* note 1.

determined that the systems accessed included systems that stored PII, including first and last names and Social Security numbers.[10]

101. Academy's Notice omits pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiffs and Class members of the Data Breach, how it determined that the PII had been accessed, and of particular importance to Plaintiffs and Class members, what actual steps Academy took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks. To date, these omitted details have not been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their PII remains protected.

102. Based on Academy's acknowledgment that "an unauthorized third party accessed and disabled some of [its] systems" and determined that the unauthorized third party had access to certain "personal information during this incident," it is evident that unauthorized criminal actors did in fact access Academy's network and exfiltrate Plaintiffs' and Class members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.

103. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have accessed Plaintiffs' and Class members' PII.

104. The Data Breach reportedly impacted the PII of approximately 284,443 individuals.[11]

[10] *Id.*
[11] *Id.*

105. Stunningly, approximately 9,300 credentials—of the current and former employees of Academy—have been published on the Dark Web and are available to download. These credentials include, *inter alia*, full names, email addresses (which use the email domain "@academymortgage.com"), employee titles, phone numbers, social media ID numbers (including Facebook, Twitter, LinkedIn, and Instagram), usernames, user ID numbers, passwords, hashed passwords, and IP addresses.

106. The metadata of these exposed credentials reveal that the earliest "date_added" was January 1, 2020. Thus, on information and belief, ALPHV BlackCat committed the Data Breach by using the exposed credentials of Academy's current and former employees.

ALPHV BlackCat Publishes PII on the Dark Web

107. On May 14, 2023, the notorious cybercriminal group "ALPHV BlackCat" revealed that it had exfiltrated PII from Academy during the Data Breach.[12] In particular, ALPHV BlackCat posted on its Dark Web website the following:

a. "We have been in your network for a long time and have had time to study your business."[13]

b. "In addition, we have stolen your confidential data and are ready to publish it."[14]

[12] *See also Academy Mortgage*, BREACHSENSE (May 15, 2023) https://www.breachsense.com/breaches/academy-mortgage-data-breach/; Vishwa Pandagle, *BlackCat Ransomware Claims Academy Mortgage Cyber Attack*, THE CYBER EXPRESS (May 15, 2023) https://thecyberexpress.com/academy-mortgage-cyber-attack-blackcat/.
[13] FalconFees.io (@FalconFeedsio), X, (May 15, 2023, 4:30 AM) https://x.com/FalconFeedsio/status/1658042032672104449/.
[14] *Id*.

c. "We have your customer/partner data, personal data, finances, confidential data and so on."[15]

108. Thereafter, ALPHV BlackCat updated its Dark Web website and declared the following:

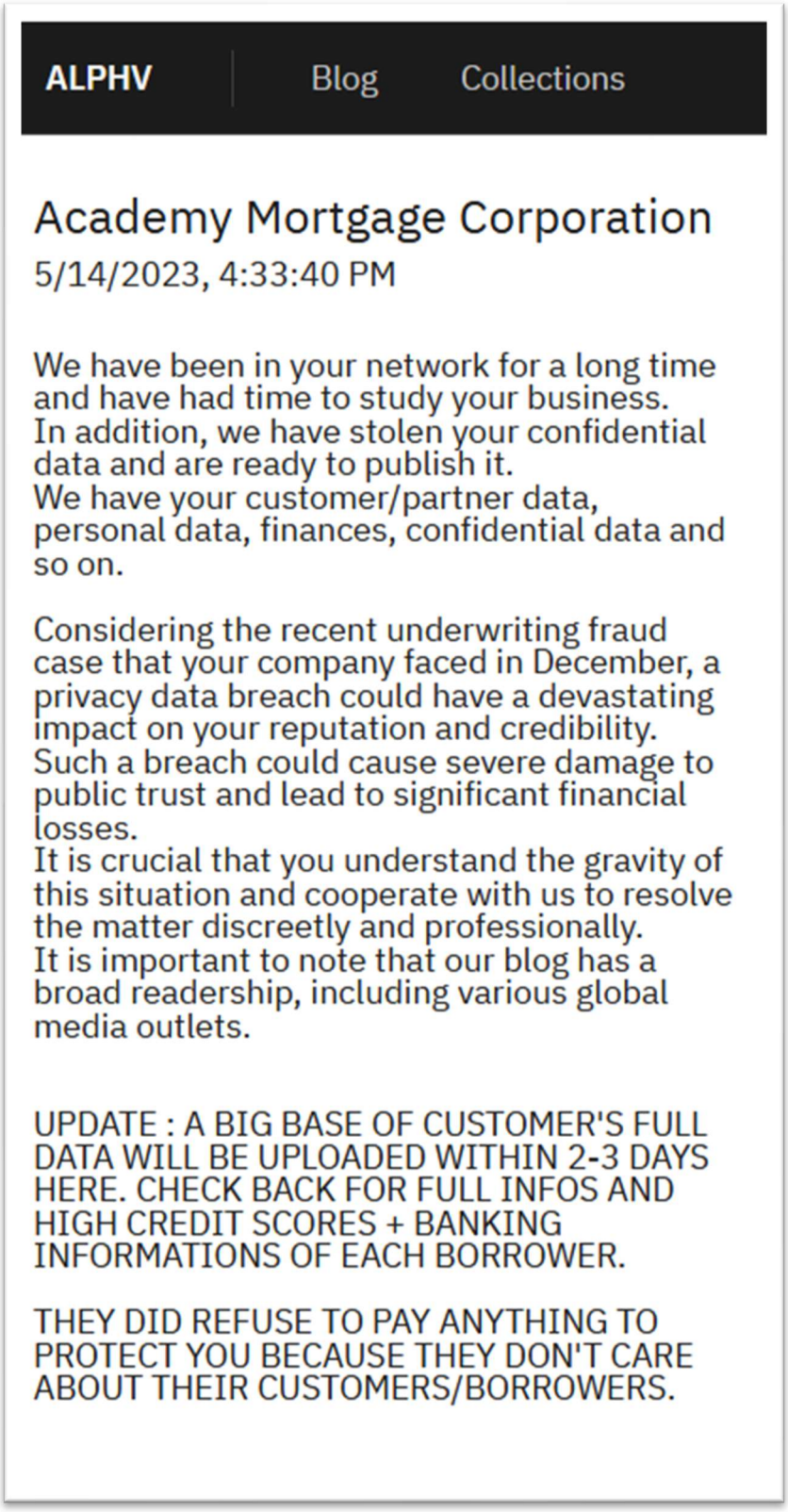
a. "UPDATE: A BIG BASE OF CUSTOMER'S FULL DATA WILL BE UPLOADED WITHIN 2-3 DAYS HERE."[16]

b. "CHECK BACK FOR FULL INFOS AND HIGH CREDIT SCORES + BANKING INFORMATIONS OF EACH BORROWER."[17]

c. "THEY DID REFUSE TO PAY ANYTHING TO PROTECT YOU BECAUSE THEY DON'T CARE ABOUT THEIR CUSTOMERS/BORROWERS."[18]

109. A screenshot of ALPHV BlackCat's Dark Web post is provided below.[19]

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*


ALPHV
Blog
Collections
Academy Mortgage Corporation
5/14/2023, 4:33:40 PM
We have been in your network for a long time and have had time to study your business.
In addition, we have stolen your confidential data and are ready to publish it.
We have your customer/partner data, personal data, finances, confidential data and so on.
Considering the recent underwriting fraud case that your company faced in December, a privacy data breach could have a devastating impact on your reputation and credibility.
Such a breach could cause severe damage to public trust and lead to significant financial losses.
It is crucial that you understand the gravity of this situation and cooperate with us to resolve the matter discreetly and professionally.
It is important to note that our blog has a broad readership, including various global media outlets.
UPDATE : A BIG BASE OF CUSTOMER'S FULL DATA WILL BE UPLOADED WITHIN 2-3 DAYS HERE. CHECK BACK FOR FULL INFOS AND HIGH CREDIT SCORES + BANKING INFORMATIONS OF EACH BORROWER.
THEY DID REFUSE TO PAY ANYTHING TO PROTECT YOU BECAUSE THEY DON'T CARE ABOUT THEIR CUSTOMERS/BORROWERS.

110. The involvement of ALPHV Blackcat is significant—in fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about ALPHV Blackcat.[20] Specifically, the joint "Cybersecurity Advisory" (CSA) stated, *inter alia*, that:

a. "ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion."[21]

b. "This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances."[22]

c. "ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations."[23]

d. "According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments."[24]

e. "ALPHV Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access."[25]

[20] *ALPHV Blackcat*, FBI & CISA (Dec. 19, 2023) https://www.cisa.gov/sites/default/files/2023-12/aa23-353a-stopransomware-alphv-blackcat_0.pdf.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

f. "Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR, Tox, email, or encrypted applications."[26]

111. Indeed, on or around May 14, 2023, ALPHV/BlackCat then ***published*** a plethora of the exfiltrated PII on the Dark Web.[27] Numerous third-party reports confirmed the publishing of PII on the Dark Web by ALPHV BlackCat. One reporter explained that "Academy Mortgage now finds itself in the [] unenviable position of having its sensitive files ***dumped on the dark web*** by the AlphV (BlackCat) ransomware group."[28] Similarly, the industry-focused periodical "National Mortgage Professional" reported that "BlackCat steals confidential files" from Academy and "posts images of them on the dark web."[29]

112. Documents posted on the dark web from the Data Breach include completed mortgage applications, financial statements, signed and notarized mortgage documents, mortgage statements, fingerprints, signatures, driver's licenses (including several from Utah and Texas), and passports.

---

[26] *Id.*

[27] *Academy Mortgage*, RANSOMWARE.LIVE (July 26, 2023) https://www.ransomware.live/search/academy%20mortgage.

[28] *Only Months After Dealing With One Problem, Academy Mortgage Gets Hit With a Ransomware Attack*, DATABREACHES.NET, https://databreaches.net/2023/05/15/only-months-after-dealing-with-one-problem-academy-mortgage-gets-hit-with-a-ransomware-attack/ (last accessed Feb. 18, 2025) (emphasis added).

[29] David Krechevsky, *Report: Academy Mortgage Targeted By Ransomware Group*, NATIONAL MORTGAGE PROFESSIONAL (May 16, 2023) https://nationalmortgageprofessional.com/news/report-academy-mortgage-targeted-ransomware-group.

113. These documents are significant because they confirm that: (1) ALPHV BlackCat accessed and exfiltrated the PII of the Class during the Data Breach, and (2) ALPHV BlackCat published stolen PII on the Dark Web.

114. Despite the involvement of ALPHV BlackCat, Academy declined to warn Plaintiffs and Class Members until December 20, 2023—*i.e.*, a full 274 days after Academy detected the Data Breach and 220 days after ALPHV BlackCat publicly leaked stolen PII on the Dark Web.

Academy Failed to Follow FTC Guidelines

115. According to the Federal Trade Commission (the "FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has promulgated numerous guides for business which highlight the importance of implementing reasonable data security practices.

116. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

117. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

118. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

119. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

120. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

121. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. These FTC enforcement actions include actions against mortgage companies, like Defendant.

122. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[30] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

123. Defendant was at all times fully aware of its obligation to protect its customers' and employees' PII it was entrusted with. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class members.

Academy Failed to Comply with the Gramm-Leach-Bliley Act

124. Academy is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

125. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

126. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

127. The GLBA Privacy Rule became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

128. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to

December 30, 2011 and by Regulation P after that date.

129. Both the Privacy Rule and Regulation P require financial institutions to provide consumers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

130. Upon information and belief, Defendant failed to provide annual privacy notices to consumers after the relationship ended, despite retaining these consumers' PII and storing that PII on Defendant's network systems.

131. Defendant failed to adequately inform their consumers that they were storing and/or sharing, or would store and/or share, the consumers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the relationship ended.

132. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of

consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

133. As alleged herein, Defendant violated the Safeguards Rule.

134. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of consumer information.

135. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class members with a non-affiliated third party without providing Plaintiffs and Class Member (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Academy Failed to Comply with Industry Standards for Data Security

136. Experts studying cyber security routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

137. Several best practices have been identified that at a minimum should be implemented by corporate entities like Defendant, including but not limited to: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

138. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

139. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

140. These foregoing frameworks are existing and applicable industry standards in the corporate industry and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

Academy Owed Plaintiffs and Class Members a Duty to Safeguard Their PII

141. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and

requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class members.

142. Defendant owed a duty to Plaintiffs and Class members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

143. Defendant owed a duty to Plaintiffs and Class members to implement processes that would detect a compromise of PII in a timely manner.

144. Defendant owed a duty to Plaintiffs and Class members to act upon data security warnings and alerts in a timely fashion.

145. Defendant owed a duty to Plaintiffs and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

146. Defendant owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices.

Academy Knew that Criminals Target PII

147. It is well known, especially in Defendant's industry, that PII, including Social Security Numbers, is an invaluable commodity and a frequent target of hackers. Data breaches, including those perpetrated against mortgage companies that store PII in their systems, have become widespread.

148. In the third quarter of the 2023 fiscal year alone, 733 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[31]

[31] *See ITRC Q3 Data Breach Analysis*, Identity Theft Resource Center, https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed July 16, 2024).

149. Additionally, as companies became more dependent on computer systems to run their businesses, *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of Things, the danger posed by cyber criminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[32]

150. Indeed, cyberattacks have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[33]

151. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[34]

152. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health

[32] *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PICUS (March 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.
[33] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[34] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[35]

153. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[36]

154. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published an online "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.[37]

155. In light of these warnings, and the recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

---

[35] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services (Apr. 22, 2014), https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[36] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNet (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

[37] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed Sep. 4, 2023).

156. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

157. At all relevant times, Defendant knew, or should have known, that Plaintiffs', and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Defendant should have anticipated and guarded against.

158. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII belonging to Academy's customers and employees, like Plaintiffs and Class members.

PII is Inherently Valuable

159. PII is a valuable property right.[38] The value of PII as a commodity is measurable.[39] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[40] American companies are estimated to have spent over $19 billion on acquiring

[38] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").
[39] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.
[40] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, p.4, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[41] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

160. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

161. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.

162. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[42] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[43] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[44] Criminals can also purchase access to entire company data

---

[41] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[42] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[43] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[44] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

breaches from $900 to $4,500.[45] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[46]

163. Criminals can use stolen PII to extort a financial payment by "leveraging details specific to a disease or terminal illness."[47] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[48]

164. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[49]

165. Further, an active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[50]

166. In fact, the data marketplace is so sophisticated that consumers can actually sell

---

[45] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Feb. 20, 2025).
[46] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[47] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[48] *Id.*
[49] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.
[50] See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[51]

167. As a result of the Data Breach, Plaintiffs' and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

168. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

169. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[52]

170. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[53] Experian, one of the largest credit reporting companies

[51] *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, Los Angeles Times (Nov. 5, 2019 5:00 AM PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[52] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Feb. 20, 2025).

[53] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or

in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[54]

171. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[55]

172. Moreover, Social Security Numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's SSN, as experienced by Plaintiffs and Class members, can lead to identity theft and extensive financial fraud:

> "A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

---

identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[54] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[55] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Feb. 20, 2025).

> illegally using your Social Security number and assuming your identity can cause a lot of problems."[56]

173. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

174. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[57]

175. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and class members.

---

[56] *Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 20, 2025).

[57] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-shackers-has-millionsworrying-about-identity-theft.

176. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black-markets for years.

177. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

178. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[58]

179. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[59]

180. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

181. One such example of criminals using PII for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

[58] Ari Lazarus, *How fast will identity thieves use stolen info?*, Federal Trade Commission (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[59] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

182. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

183. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[60]

184. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

185. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I

[60] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[61]

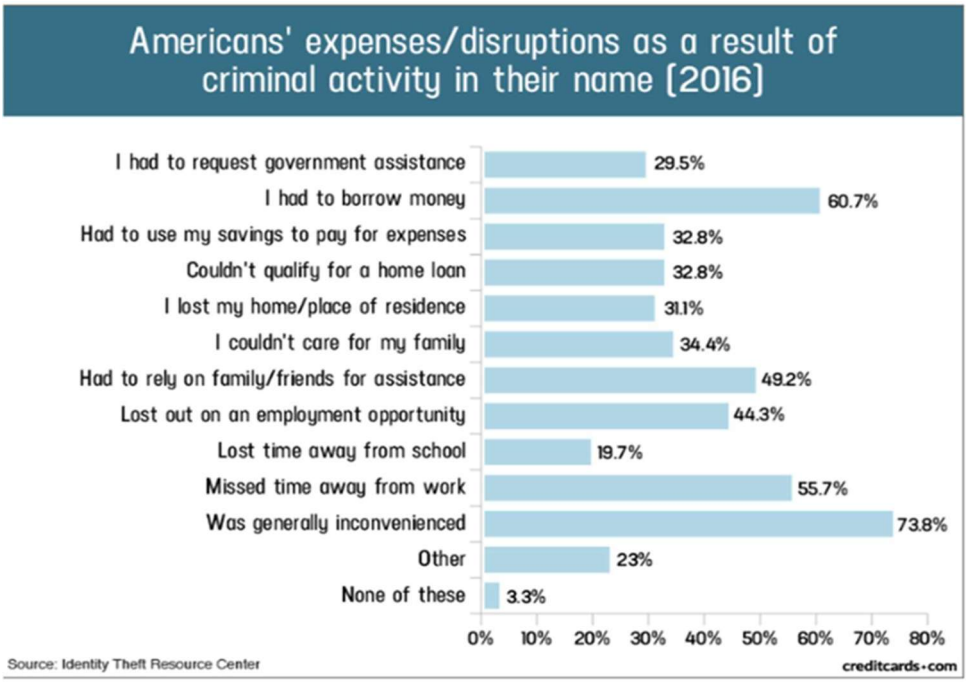
186. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

187. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[62]

188. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

189. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

[61] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[62] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



190. Victims of the Data Breach, like Plaintiffs and Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[63]

191. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

[63] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

192. Plaintiffs and Class members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

193. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the

implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown to be incapable of protecting Plaintiffs' and Class members' PII.

The Data Breach Was Foreseeable and Preventable

194. Data disclosures and data breaches are preventable.[64] As Lucy Thomson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[65] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[66]

195. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[67]

196. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[68]

197. Plaintiffs and Class members entrusted their PII to Defendant as a condition of receiving mortgage services. Plaintiffs and Class members understood and expected that

[64] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thomson, ed., 2012).
[65] *Id.* at 17.
[66] *Id.* at 28.
[67] *Id.*
[68] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Feb. 20, 2025).

Defendant or anyone in Defendant's position would safeguard their PII against cyberattacks, delete or destroy PII that Defendant was no longer required to maintain, and timely and accurately notify them if their PII was compromised.

Damages Sustained by Plaintiffs and Class Members

198. To date, Defendant has done nothing to provide Plaintiffs and Class members with relief for the damages they have suffered as a result of the Data Breach. Academy only offered "Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score" for a mere "twelve (12) months from the date of enrollment,"[69] but did not disclose how it determined eligibility. Not only did Defendant fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services does nothing to compensate Class members for damages incurred and time spent dealing with the Data Breach.

199. Plaintiffs and Class members have been damaged by the compromise of their PII in the Data Breach.

200. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

201. Plaintiffs and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class members.

[69] *See Notice of Data Security Incident*, *supra* note 1.

202. Plaintiffs and Class members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

203. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security numbers, insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

204. Plaintiffs and Class members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their PII, a form of property that Academy obtained from Plaintiffs and Class members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

205. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

206. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class members to take the following measures to protect themselves: "[y]ou should always remain vigilant and monitor your accounts for suspicious or unusual activity."

207. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, researching online how to protect themselves from fraud and identity theft, signing up for the credit monitoring and identity theft insurance services offered by Defendant, contacting law enforcement regarding suspicious calls, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

208. Plaintiffs' mitigation efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their

credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[70]

209. Class members who experience actual identity theft and fraud will need to spend time and money fixing the problem and repairing their good name.

210. Further, as a result of Defendant's conduct, Plaintiffs and Class members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

211. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

212. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online, is properly encrypted, and that access to such data is password protected.

213. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures and protocols that were necessary to protect Plaintiffs' and Class members' PII.

214. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

[70] See Identity Theft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 20, 2025).

215. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiffs' and Class members' PII were stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of the breach.

216. The risk of improper disclosure of Plaintiffs' and Class members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' PII from that risk left the PII in a dangerous condition.

217. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

218. Plaintiffs bring this class action on behalf of themselves and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

> **Nationwide Class**
> All persons residing in the United States whose PII was compromised in the Data Breach disclosed by Defendant on or about December 20, 2023, including all who were sent notice of the Data Breach (the "Class").

219. Plaintiffs also bring this class action on behalf of the following subclasses:

> **Washington Subclass**
> All persons residing in the state of Washington whose PII was compromised in the Data Breach disclosed by Defendant on or about December 20, 2023,

including all who were sent notice of the Data Breach (the "Washington Subclass").

Idaho Subclass
All persons residing in the state of Idaho whose PII was compromised in the Data Breach disclosed by Defendant on or about December 20, 2023, including all who were sent notice of the Data Breach (the "Idaho Subclass").

220. Excluded from the Class are Academy Mortgage Corporation and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

221. Plaintiffs reserve the right to amend the definitions of the Class or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

222. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

223. **Numerosity:** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Academy reported to the Office of the Maine Attorney General that approximately 284,443 individuals' information was exposed in the Data Breach.71

224. **Ascertainability:** Class members are readily identifiable from information in Defendant's possession, custody, and control.

225. **Commonality:** Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

[71] *Notice of Data Security Incident*, *supra* note 1.

a. Whether Academy had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

b. Whether Academy's computer systems and data security practices used to protect Plaintiffs' and Class members' PII violated the FTC Act and/or state laws and/or Academy's other duties discussed herein;

c. Whether Academy failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class members;

d. Whether Plaintiffs and Class members suffered injury as a proximate result of Academy's negligent actions or failures to act;

e. Whether Academy failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

f. Whether an implied contract existed between Class members and Academy providing that Academy would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class members;

h. Whether Academy's actions and inactions alleged herein constitute gross negligence;

i. Whether Academy breached its duties to protect Plaintiffs' and Class members' PII; and

j. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

226. Academy engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

227. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Academy, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

228. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

229. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Academy, so it would be

impracticable for Class members to individually seek redress from Academy's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

230. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

231. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

232. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

233. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

234. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

235. Academy requires its customers, including Plaintiffs and Class members, to submit non-public PII in the ordinary course of providing its mortgage and loan services.

236. Academy gathered and stored the PII of Plaintiffs and Class members as part of its business of soliciting its services to customers.

237. Plaintiffs and Class members entrusted their PII to Academy on the premise and with the understanding that it would safeguard their PII, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

238. By assuming the responsibility to collect and store this PII, Academy owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control. This duty includes, but is not limited to (1) exercising reasonable care in handling and using the PII in its care and custody; (2) implementing industry-standard security procedures sufficient to reasonably protect the PII from a data breach, theft, or unauthorized access; (3) promptly detecting attempts at unauthorized access; (4) notifying Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII; and (5) exercising appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

239. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA was intended to protect. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against. Defendant violated Section 5 of the FTCA by failing to adequately safeguard Plaintiffs' and Class members' PII.

240. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains

reasonable administrative, technical, and physical safeguards. Plaintiffs and Class members are within the class of persons that the GLBA was intended to protect. The harm occurring as a result of the Data Breach is the type of harm that the GLBA intended to guard against. Defendant violated the GLBA by failing to adequately safeguard Plaintiffs' and Class members' PII.

241. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Academy and Plaintiffs and Class members. That special relationship arose because Plaintiffs and the Class members entrusted Academy with their confidential PII, a necessary part of being customers at Defendant.

242. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

243. Academy knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class members' PII and the importance of maintaining secure systems and using encryption, which it did not use. Academy knew, or should have known, of the many data breaches that targeted corporate entities in recent years.

244. Given the nature of Academy's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, it should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

245. Academy breached these duties by:

a. failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes,

controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiffs and Class members PII;

d. failing to detect, in a timely manner, that Plaintiffs' and Class members' PII had been compromised;

e. failing to remove former customers' PII it was no longer required to retain pursuant to regulations from its systems;

f. failing to timely and adequately notify Plaintiffs and Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the Data Breach.

246. It was reasonably foreseeable to Academy that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

247. But for Academy's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

248. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages.

249. As a result of Academy's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (vii) actual or attempted fraud; (viii) invasion of privacy; (ix) statutory damages; (x) nominal damages; and (xi) the continued increased risk to their PII.

250. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

251. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

252. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

253. Plaintiffs and Class members delivered their PII to Defendant as part of the process of obtaining services provided by Defendant.

254. Plaintiffs and Class members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if and when their PII had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class members' PII in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

255. In providing their PII, Plaintiffs and Class members entered into an implied contract with Defendant, whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class members' PII.

256. Implicit in the agreement between Plaintiffs and Class members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

257. In delivering their PII to Defendant, Plaintiffs and Class members intended and understood that Defendant would adequately safeguard that data.

258. Plaintiffs and the Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

259. Defendant accepted possession of Plaintiffs' and Class members' PII.

260. Had Defendant disclosed to Plaintiffs and Class members that Defendant did not have adequate computer systems and security practices to secure consumers' PII, Plaintiffs and Class members would not have provided their PII to Defendant.

261. Defendant recognized that consumers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class members.

262. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

263. Defendant breached the implied contract with Plaintiffs and Class members by failing to take reasonable measures to safeguard their data.

264. Defendant breached the implied contract with Plaintiffs and Class members by failing to promptly notify them of the access to and exfiltration of their PII.

265. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic

costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiffs and Class members were deprived of the data protection and security that Defendant promised when Plaintiffs and the Class members entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiffs' and Class members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class members' PII.

266. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

267. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

269. This claim is pleaded in the alternative to the breach of implied contract claim.

270. Plaintiffs and Class members conferred a monetary benefit upon Academy in the form of monies paid for mortgage services or through labor. In exchange, Plaintiffs and Class members should have received from Academy the services that were the subject of the transaction and should have had their PII protected with adequate data security.

271. Academy accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members. Academy also benefitted from the receipt of Plaintiffs' and Class members' PII.

272. Academy knew that Plaintiffs and Class members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Academy profited from Plaintiffs' and Class members' collected and retained data and used Plaintiffs' and Class members' PII for business purposes.

273. As a result of Academy's conduct, Plaintiffs and Class members suffered actual damages.

274. Academy should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

275. Academy should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

276. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

277. Plaintiffs and the Class members had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

278. The State of Utah recognizes the tort of Invasion of Privacy:

> The elements of an invasion-of-privacy claim are: (1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities. Shattuck-Owen v. Snowbird Corp, 2000 UT 94, 16 P.3d 555 (2000) (citing Stein v. Marriott Ownership Resorts, Inc., 944 P.2d 374, 380 (Utah Ct.App.1997) (quoting W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 856-57 (5th ed.1984) (footnote omitted)).

279. Defendant owed a duty to its consumers, including Plaintiffs and the Class members, to keep this information confidential.

280. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class members' PII is highly offensive to a reasonable person.

281. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class members disclosed their sensitive and confidential information to Defendant as part of seeking Defendant's services, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

282. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

283. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

284. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

285. Defendant had notice and knew or should have known that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class members.

286. As a proximate result of Defendant's acts and omissions, the PII of Plaintiffs and Class members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class members to suffer damages.

287. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class members because their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

288. Plaintiffs and the Class members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class members.

289. In addition to injunctive relief, Plaintiffs, on behalf of themselves and Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
RCW §§ 19.86.010 *et seq.* ("WCPA")
(On Behalf of Plaintiffs Allen and Smith and the Washington Subclass)

290. Plaintiffs Allen and Smith reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

291. Plaintiffs Allen and Smith and Academy are "persons" under the WCPA. RCW § 19.86.010(1).

292. Academy's sale of services to Plaintiffs Allen and Smith and all other Washington Subclass members constitutes "trade" or "commerce" under the WCPA. RCW § 19.86.010(2).

293. The WCPA states, "Unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce are hereby declared unlawful." RCW § 19.86.020. Academy's failure to adequately safeguard Plaintiffs Allen's and Smith's and all other Washington Subclass members' PII while representing that their PII would be protected is an "unfair or deceptive practice" under the WCPA.

294. Academy's failure to adequately safeguard Plaintiffs Allen's and Smith's and Washington Subclass members' PII is injurious to the public interest pursuant to RCW § 19.86.093(3)(a) because Academy's actions not only harmed Plaintiffs Allen and Smith, but harmed hundreds of thousands of other persons.

295. Had Plaintiffs Allen and Smith and Washington Subclass members been aware of the omitted and misrepresented facts, i.e., that Academy would not adequately protect their PII, Plaintiffs Allen and Smith and Washington Subclass members would not have sought services from Academy.

296. Pursuant to RCW § 19.86.090, Plaintiffs Allen and Smith seek actual and treble damages on behalf of themselves and all other Washington Class members.

COUNT VI
VIOLATION OF THE IDAHO CONSUMER PROTECTION ACT
Idaho Code §§ 48-601 *et seq.* ("ICPA")
(On Behalf of Plaintiff Kucherry and the Idaho Subclass)

297. Plaintiff Kucherry realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

298. Plaintiff Kucherry and Academy are "persons" under the ICPA. I.C. § 48-602(1).

299. Academy's sale of services to Plaintiff Kucherry and all other Idaho Subclass members constitutes "trade" or "commerce" under the ICPA. I.C. § 48-602(2).

300. The ICPA lists 19 unfair methods of competition and unfair or deceptive acts or practices. Academy's failure to adequately safeguard Plaintiff Kucherry's and all other Idaho Subclass members' PII while representing that their PII would be protected is an "unfair or deceptive practice" under at least the following provisions of the ICPA:

a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have." I.C. § 48-603(5);

b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." I.C. § 48-603(7);

c. "Advertising goods or services with intent not to sell them as advertised." I.C. § 48-603(9);

d. "Engaging in any act or practice that is otherwise misleading, false, or deceptive to the consumer." I.C. § 48-603(17); and

e. "Engaging in any unconscionable method, act or practice in the conduct of trade or commerce." I.C. § 48-603(18).

301. Had Plaintiff Kucherry and Idaho Subclass members been aware of the omitted and misrepresented facts, i.e., that Academy would not adequately protect their PII, Plaintiffs Kucherry and Idaho Subclass members would not have sought services from Academy.

302. Pursuant to I.C. § 48-608, Plaintiff Kucherry seeks actual damages or $1,000, whichever is greater, on behalf of herself and all other Idaho Class members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Academy as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Academy from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft. The injunctive relief sought includes, but is not limited to:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

d. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class members' respective lifetimes;

e. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class members;

f. prohibiting Defendant from maintaining the PII of Plaintiffs and Class members on a cloud-based database;

g. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

h. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

i. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

j. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

k. requiring Defendant to conduct regular database scanning and securing checks;

l. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

m. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

n. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

o. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

p. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

q. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

G. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 21, 2025

Respectfully submitted,

By: */s/ Brittany Resch*

Brittany Resch*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
bresch@straussborrelli.com
raina@straussborrelli.com

Andrew W. Ferich*
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
aparkhill@barnowlaw.com

Proposed Interim Class Counsel

Daniel O. Herrera**
Nickolas J. Hagman **
Alexander J. Sweatman**
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880

Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
asweatman@caffertyclobes.com

James E. Magleby (7247)
Jennifer Fraser Parrish (11207)
MAGLEBY CATAXINOS & GREENWOOD, PC
141 West Pierpont Avenue
Salt Lake City, UT 84101
Telephone: (801) 359-9000
Facsimile: (801) 359-9011
magleby@mcg.law
parrish@mcg.law

Jason R. Hull [11202]
Trevor C. Lang [14232]
MARSHALL OLSON & HULL, PC
Newhouse Building
Ten Exchange Place, Suite 350
Salt Lake City, Utah 84111
Telephone: (801) 456-7655
jhull@mohtrail.com
tlang@mohtrial.com

*admitted *pro hac vice*
** *pro hac vice* forthcoming

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, Brittany Resch, hereby certify that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 21st day of February, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Brittany Resch*

Brittany Resch
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
bresch@straussborrelli.com